EMBEDDED MULTI-MODEL BIOMETRIC AUTHENTICATION FRAMEWORK

Sneha Kurhekar [1] | Prof. H. Upadhyay [1] , Prof. K. Sujatha [1]

[1] ENTC Department, SRCOE, Pune University, Pune, Maharashtra, India.

ABSTRACT

Today, biometric authentication plays vital role in the social and commercial area. This paper proposed a securing system access using multi-model biometrics for authorization with the embedded platform. It consists of the embedded system to verify the signatures, fingerprint and key pattern for authentication of user. Proposed system works in two phases of authentication i.e enrollment phase and evaluation phase. In enrollment phase all authentication factors are stored in data base and in evaluation phase stored one is compared with tested parameters. In proposed system HMM is implemented on android side for the signature, DTW is implemented on controller side for fingerprint and key pattern is with FPGA. Thus proposed work gives the two factor authentication biometric system with extra layer of security.

KEYWORDS: Embedded System; Biometrics; FPGA; DTW and HMM model.

I. Introduction

Day by day, natural and secure access to interconnected systems is becoming more and more important. Fingerprint and signature are the most pervasive methods of individual identification and document authentication. Authentication of a person's identity is a need in many social and commercial interactions. It is also necessary to verify people identity in a fast, easy to use and user-friendly way. Because of this, biometric solutions are considered one of the most trusted and natural ways of identifying a person and controlling access to systems and applications. On the basis of the input acquisition method, it can be categorized into static verification technique (offline) and dynamic verification technique (online). There are many more other personal authentication techniques as well. Some of them uses the possession of the token (i.e ID cards) and some of them are knowledge based (i.e password, key-phase etc). But, the token based technique whose attributes can be stolen or lost whereas knowledge based approaches whose attributes can be forgotten, which become major drawback of such techniques. But the biometrics attributes, do not suffer from such disadvantages.

To the best of our knowledge, proposed biometric model gives the proper authentication with extra layer of security. We are used both traits of biometrics physiological trait fingerprint and behavioural trait signature. So, we say proposed system is a multi-model biometric system. Toward these direction the contribution of these paper is three fold: First we are using signature (behavioural trait), secondly fingerprint (biological trait) and lastly key pattern. When all these three parameters matches then and only then user get authorized. Proposed system is used Two-factor authentication process. Proposed biometric authentication system built up by knowledge factor (key pattern) and inherence factor (signature and fingerprint). Proposed system is the dynamic verification technique. This paper is organized as follows. Section II describes the architecture of the multimodal biometric system. Section III presents working of proposed system. Section IV shows implementation of proposed system: Section V presents result and discussion and finally Section VI presents the conclusions.

II. Architecture of Proposed System

Fig. 1 shows the architecture adopt by proposed system which having generic architecture as a basic platform with some additional advantages features. Main building blocks of the architecture are listed below. As shown in fig 7. there are wireless connections in between Android and Matlab. Connection between android and Matlab is created through Wi-Fi. Matlab and microcontroller are connected through RS 232. Finger print module R302 is connected to microcontroller with serial port and microcontroller is connected to FPGA through 8 wire connection.

A. Android phone

We are using android phone as a data acquisition element for the user signature. In android, a touch gesture occurs when a user places one or more fingers on the touch screen, and application interprets that pattern of touches as a particular gesture. The gesture starts when the user first touches the screen, continues as the system tracks the position of the user's finger(s), and ends by capturing the final event of the user's fingers leaving the screen. Android provides the Gesture detector class for detecting common gestures.

B. Finger print module R302

This is a finger print sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person.

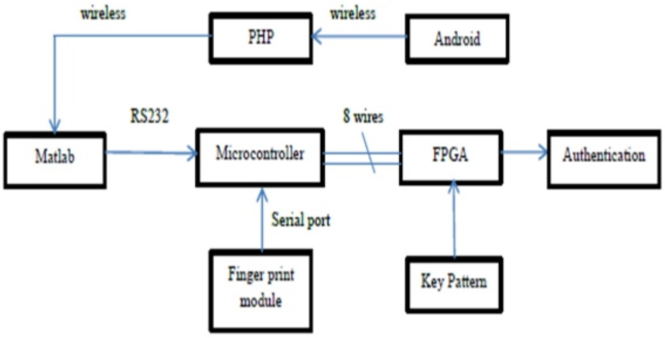


Fig.1. Architecture of proposed Multimodal biometric system

C. MATLAB

MATLAB is a high- performance language for technical computing. It integrates computation, visualization and Programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. MATLAB is complemented by family of application specific solutions called toolboxes. The signal Processing Toolbox is a collection of MATLAB functions (called M-functions or M-files) that extend the capability of the MATLAB environment for the solution of digital image processing problems

D. Microcontroller (ATmega162v-8PI)

We are using microcontroller Atmega162V-8PI. It is a High-performance, Low-power AVR® 8-bit Microcontroller. The ATmega162 is a low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega162 achieves throughputs approaching 1 MIPS per MHz allowing the system designer to optimize power consumption versus processing speed.

E. Key pattern

In proposed system we are using key pattern as a third parameter of authentication. Here we are implemented key pattern with help of FPGA. We are taking LSB as key pattern, so N number of users can be enrolled and authenticated by using proposed system. On the other hand, for the key pattern the last 3 bits of the ID will be used. Key pattern is based on the user ID. In proposed system, first three data pins (D0, D1 and D2) of microcontroller is for the in-code pattern whereas next three pins (D4,D5,D6) are used for key pattern and last pin D7 is used for showing the result of key pattern matching. If we get 1 in pin D7 it means key pattern is matched and if we get 0 as a output at pin D7 it means key pattern is not matched.

F. FPGA

A field-programmable gate array (FPGA) is an integrated circuit designed to be configured by a customer or a designer after manufacturing – hence "field-programmable". The FPGA configuration is generally specified using a hardware description language (HDL), similar to that used for an application-specific integrated circuit (ASIC). FPGAs contain an array of programmable logic blocks, and a hierarchy of reconfigurable interconnects that allow the blocks to be "wired together", like many logic gates that can be inter-wired in different configurations.

III. Working of Proposed System

A. Data Acquisition

Data acquisition is the process of collecting input data from input devices. So signatures are collected using android mobile phone whereas finger prints are collected from the Finger Print Sensor R305.

B. Image pre-processing

Pre-processing stage is used to reduce the noise and normalized the images obtained from input devices. The pre-processing stage is enclosed by normalization, segmentation, filtering like processes. Binarization and thinning process are carried out over the finger print image in the pre-processing stage.

C. Feature Extraction

Feature extraction is the efficiency measure tool for the signature verification process. Proposed system, deals with the dynamic features and used function based features as signature is characterized in terms of time function. Dynamic features are extracted from signatures that are acquired in real time which make the signature more unique. In proposed system, we are going to deal with the some features like thinning of images, perimeter, area, orientation, eccentricity etc. Pattern of interleaved ridges and valleys lines can be described by a fingerprint image. Minutia is the unique feature of the ridges. Minutia points occur at ridges bifurcation. Bifurcation is the process where a ridge split into two lines at specific points. The feature extraction of fingerprint will consist of finding the ridge ending and ridge bifurcations from the input fingerprint images; begin each minutia described by its location and orientation. The final ridge structure will be used to generate feature vector know as minutiae, which will characterized the fingerprint. This will be template formed by a list of minutiae and a list of number of ridges between each pair of minutiae, and it will be stored by the system.

D. Classification

In verification process, authentication of signature, fingerprint and key pattern are done. In these, the features of signature and finger print and key pattern which stored in dada based during enrolment stage are matched with test signature, fingerprint and key pattern. K nearest neighbours (KNN) classifier used for the classification stage. The K-nearest-neighbour (KNN) algorithm measures the distance between a query scenario and a set of scenarios in the data set.

1. Distances:

We can compute the distance between two scenarios using some distance function *d(x, y)* where x, y are scenarios composed of *N* features, such that, $x = (x_1 \ldots\ldots\ldots\ldots x_N)$ and $y = (y_1 \ldots\ldots\ldots y_N)$. Two distance functions are discussed in this summary:

Absolute distance measuring: Equation 1

$$d_A(x, y) = \sum_{i=1}^{N} |x_i - y_i|$$

Euclidean distance measuring: Equation 2

$$d_E(x, y) = \sum_{i=1}^{N} \sqrt{x^2{}_i - y^2{}_i}$$

Because the distance between two scenarios is dependent of the intervals, it is recommended that resulting distances be scaled such that the arithmetic mean across the dataset is 0 and the standard deviation 1. This can be accomplished by replacing the scalars with according to the following function:

$$x^1 = \frac{x - \bar{x}}{\sigma(x)}$$

Equation 3

Where x is the unscaled value, $\bar{x}$ is the arithmetic mean of feature x across the data set (Equation 4), $\sigma(x)$ is its standard deviation (see Equation 5), x' and is the resulting scaled value. The arithmetic mean is defined as:

$$\bar{x} = \frac{1}{N} \sum_{i=1}^{N} x_i$$

Equation 4

We can then compute the standard deviation as follows:

$$\sigma(x) = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (x_i - \bar{x})^2}$$

2. Distance functions (K-nearest-neighbour):

As stated previously, we are only considering absolute (Equation 1) and Euclidean (Equation 2) distance functions d(x, y). However, we may choose to provide the original unscaled values, or use transforms them using the scaling function in Equation 3. Now that we have established a measure in which to determine the distance between two scenarios, we can simply pass through the data set, one scenario at a time, and compare it to the query scenario. We can represent our data set as a matrix $D=N \times P$, containing P scenarios S^1 ……..S^P, where each scenario S^i contains N features $S^i=\{S_i^1, \ldots\ldots\ldots\ldots S_n^i\}$ A vector o with length P of output values accompanies this matrix, listing the output value o^i for each scenario s^i. It should be noted that the vector o can also be seen as a column matrix; if multiple output values are desired, the width of the matrix may be expanded.

KNN can be run in these steps:

1. Store the output values of the M nearest neighbors to query scenario q in vector $r=\{r^1, \ldots \ldots, r^M\}$ by repeating the following loop times:

a. Go to the next scenario Si in the data set, where i is the current iteration within the domain
{1,…….., P}

b. If is not set or $q < d(q, S^i): q \leftarrow d(q, s^i), t \leftarrow o^i$

c. Loop until we reach the end of the data set (i.e. i = P).

d. Store q into vector c and t into vector r.

2. Calculate the arithmetic mean output across as follows:

$$\bar{r} = \frac{1}{M} \sum_{i=1}^{M} r_t$$

3. Return $\bar{r}$ as the output value for the query scenario q.

IV. Implementation of Proposed System

To establish the experimental setup make all the connections as shown in fig 4. Firstly environment connection is necessary to make the wireless connection for that purpose we are using Wi- Fi connection. Afterword move toward evaluation phase in which user must enrol him/her to the system by using signature and fingerprint. This information of the user stored in the data base in enrollment phase. Next in evaluation phase test signature, fingerprint and key pattern are compared with previously stored one. Proposed system setup works in real in three phases:

A. Pre saving of segmentation on android
B. User Registration
C. User Evaluation

A. Pre saving of segmentation on android: In gesture builder library emulator save the gesture file. It provide extra layer of security.

B. User Registration: User draw the sign on the android phone it followed by fingerprint scan on the module R302. Both the input saves to the data base. Key pattern also generated by the user. All these three data are saved by user name on knowledge base.

C. User Evaluation: As we know, authentication process consists of two phase, enrollment phase and verification phase. We finish enrollment phase through the user registration. Now whatever data we are needed for evaluation i.e signature, fingerprint and key pattern is already stored in data base. Here we compare previously stored user data with newly enrolled if all the parameters matches then we get the proper authentication result.

1.Signature process:

For the signature, we are using android phone as a input. Wireless connection should be created between Android phone and Matlab. The gesture file which is created when user touches the screen and it gets stored in Matlab. Android provides the Gesture Detector class for detecting common gestures. A Hidden Markov Modelling (HMM) is used with the signature process. Knn classifier is used for classification. K nearest neighbours is a simple algorithm that stores all available cases and classifies new cases based on a similarity measure. A case is classified by a majority vote of its neighbours, with the case being assigned to the class most common amongst its K nearest neighbours measured by a distance function. If K = 1, then the case is simply assigned to the class of its nearest neighbour.

2. Fingerprint process:

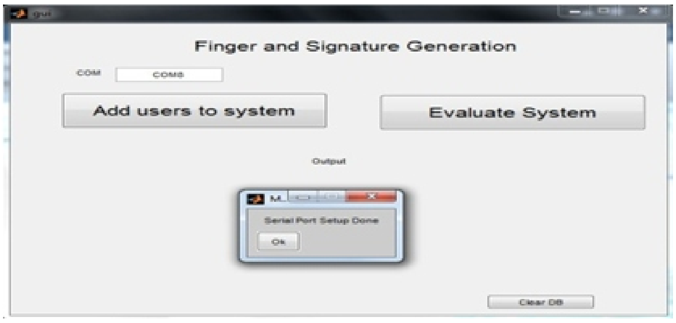
For fingerprint in proposed system we are using finger print sensor module R305. In terms of applications, there are two kinds of fingerprint recognition systems: verification and identification. In verification, the input is a query fingerprint and an identity (ID), the system verifies whether the ID is consistent with the fingerprint. The output is an answer of yes or no. The output is a short list of fingerprints. Generally, fingerprint-matching algorithms have two steps: (1) align the fingerprints and (2) find the correspondences between two fingerprints. Dynamic timing wrapping is implemented on fingerprint for the feature extraction. It involves extraction of minutia points from ridges. Dynamic time warping (DTW) is an algorithm for measuring similarity between two temporal sequences which may vary in time. DTW is a method that calculates an optimal match between two given sequences (e.g. time series).

- Two time series Q & C.
  $Q = q_1, q_2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots q_n$
  $C = c_1, c_2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots c_n$
- Construct $m \times n$ matrix D with distances $D_{ij} = d(q_i, c_j)$
- Warping path W is a contiguous set of matrix elements $W_k = (i, j)_k$
- Find : DTW $(Q, C) = min \sqrt{\sum Wk}$

In minutiae extraction identification systems minutiae considered are ridge bifurcations and terminations. Whereas in neighbourhood extraction list of minutiae neighbours is extracted for each minutia. The minutiae are ordered according to the increasing distance from the image centre and each list is ordered according to the increasing distance from the corresponding minutiae. The image centre is assumed to be the mass-centre of the detected minutiae. The minutiae list provides information on the minutiae position and on the ridge/valley behaviour between minutiae. For this reason, the line connecting each minutiae and one of its neighbours is traced, and the grey values extracted.

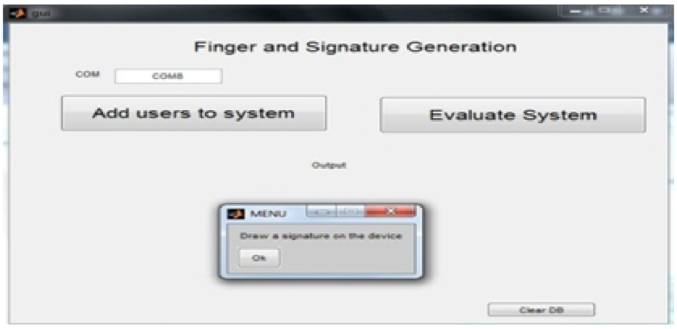
The complete embedded system works in two phases of authentication i.e enrollment phase and evaluation phase. In enrollment phase signature, fingerprint and user name are stored on database. In evaluation phase, system compares the user's signature; fingerprint and key pattern with previously stored one and according to that evaluation phase give its output. This system gives the correct authentication when all three parameters are matched. If system found that any among three is not matching with the previous one then we are not getting any authentication. System display the message "match not found".

We can observe the result evaluation phase and enrollment phase in following figures. As all setups are done, Wi- Fi connections are made and pre saving of segmentation on android are done the firstly our set up check whether serial port connections is done or not. For establishing serial port connection, correct com no should be placed as shown in fig 2. From fig 2, there is option for clearing data base through which user can clear data base if required.



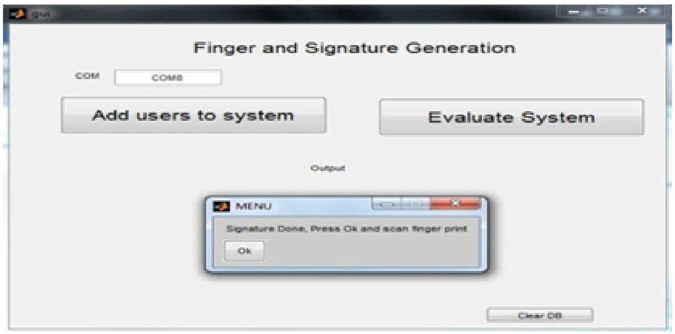
Serial Port Setup Done

Fig.2. Serial port connection



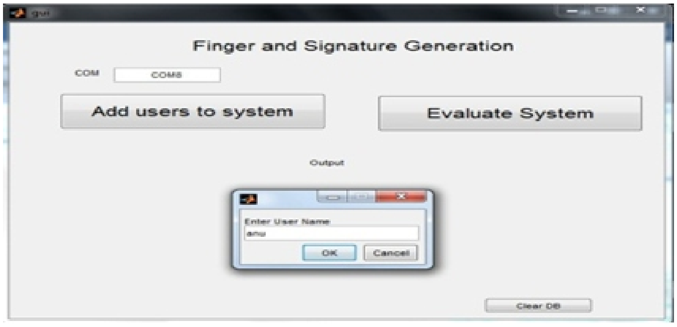
Draw a signature on the device

Fig.3 (a) Signature enrollment



Signature Done, Press Ok and scan finger print

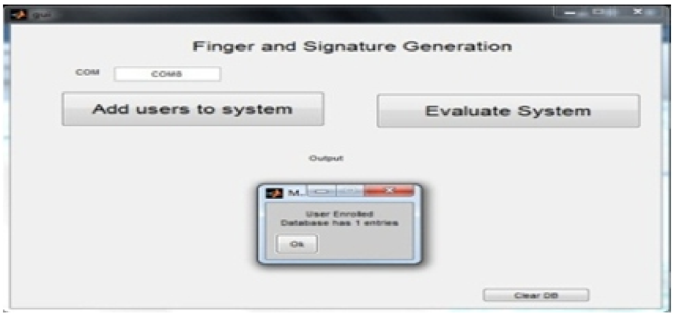
Fig. 3(b) Fingerprint enrollment



Enter User Name

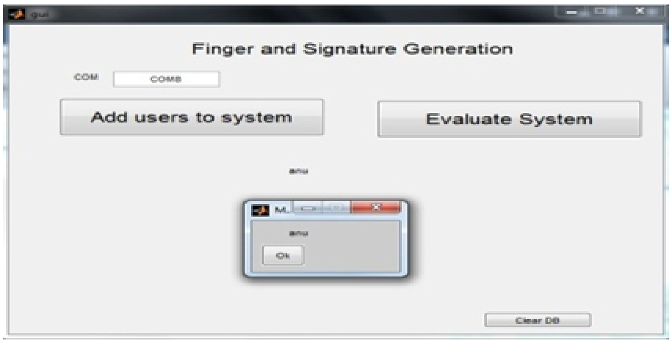
anu

Fig 3(c) Enrollment of user name



User Enrolled
Database has 1 entries

Fig. 3(d) Enrollment phase result



anu

anu

Fig 4 Authentication's result

For enrolment, user must click on "Add user to system" through which user can enroll their signature and finger print as shown in fig 3(a) and fig (b) respectively. After enrolling signature and fingerprint, user can stored that data by their name as shown in Fig 3(c). Finally fig 3(d) shows the result of enrollment process. As the enrollment phase completed, user information will be stored in data base.

In evaluation phase, classification is carried out between previously stored information with present one. Same steps are carried out for evaluation phase, same as shown in Fig. 3(a) and Fig. 3(b) and key pattern also must be entered. Finally authentication is displayed as shown in Fig 4. In following table we tabularized the result. As proposed system are used three parameters such as signature, fingerprint and key pattern. System authenticates the user only when all three parameters are matched. Table 1 represents the result of proposed system when all three parameters are matched. Table 1 shows the 7 user entry, all users are correctly implements the system then system detect the correct user every time.

Table 1: All parameters are correctly enrol

User	Actual signature	Actual fingerprint	Key pattern	System detected
User 1	User 1	User 1	1	User 1
User 2	User 2	User 2	1	User 2
User 3	User 3	User 3	1	User 3
User 4	User 4	User 4	1	User 4
User 5	User 5	User 5	1	User 5
User 6	User 6	User 6	1	User 6
User 7	User 7	User 7	1	User 7

Table 2: Result obtained by varying fingerprint

User	Actual signature	Actual fingerprint	Key pattern	System detected
User 1	User 1	User 7	1	Match not found
User 2	User 2	User 6	1	Match not found
User 3	User 3	User 5	1	Match not found
User 4	User 4	User 4	1	User 4
User 5	User 5	User 3	1	Match not found
User 6	User 6	User 2	1	Match not found
User 7	User 7	User 1	1	Match not found

Table 3: Result obtained by varying signature

User	Actual signature	Actual fingerprint	Key pattern	System detected
User 1	User 7	User 1	1	Match not found
User 2	User 6	User 2	1	Match not found
User 3	User 5	User 3	1	Match not found
User 4	User 4	User 4	1	User 4
User 5	User 3	User 5	1	Match not found
User 6	User 2	User 6	1	Match not found
User 7	User 1	User 7	1	Match not found

Table 4: Result obtained by varying key pattern

User	Actual signature	Actual fingerprint	Key pattern	System detected
User 1	User 1	User 1	0	Match not found
User 2	User 2	User 2	0	Match not found
User 3	User 3	User 3	0	Match not found
User 4	User 4	User 4	0	Match not found
User 5	User 5	User 5	0	Match not found
User 6	User 6	User 6	0	Match not found
User 7	User 7	User 7	0	Match not found

Table 2shows the result of the proposed system when we enroll fingerprint incorrectly and remaining two factors correctly. From table 2, system detects the user 4 correctly and in remaining cases it display that match not found. Table 3 also show the result with maximum accuracy in which we obtained the result by varying signature factor.

Table 5: summarized Result

User	Actual Signature	Actual fingerprint	Key pattern	System detected
User 1	User 1	User 2	0	Match not found
User 2	User 2	User 2	1	User 2
User 3	User 1	User 3	1	Match not found
User 4	User 4	User 4	1	User 5
User 5	User 5	User 5	0	Match not found
User 6	User 6	User 6	1	User 6
User 7	User 5	User 3	1	Match not found

Table 4 shows the result of proposed system by varying third factor i.e key pattern. Here we use 1 and 0 for representing correct key pattern and wrong key pattern. If result table shows 0 in key pattern column it means key pattern is not matched whereas when 1 is displayed in result table it means key pattern is matched. Table 5 shows the summary of all above result table. We can find the accuracy of system by computing the accuracy of each table. The accuracy of the system is given by the ratio of Number of correctly classified outputs to the total outputs.

Accuracy = Number of correctly classified outputs / Total outputs

For Table 2: Accuracy = 7/7=1. It means accuracy is 100%.

We can calculate the accuracy for all tables by using same formula mention above. From the above accuracy calculations we can say that proposed system is more accurate than previous one. So that we can say proposed system having lowest EER and lowest FTC.

IV. Conclusion

This paper proposed a real time authentication framework using multi-model biometrics. It consists of the embedded system to verify the signatures, fingerprint and key pattern for authentication of user. Proposed framework provides a strong user authentication solution with the extra layer of security. When a high level of security is needed, it is necessary that you combine more than one authentication factors. This work implements such a biometric system which consists of 'Physiological trait (fingerprint) as well as Behavioural trait (signature) of biometrics. The complete embedded system works in two phases of authentication i.e enrollment phase and evaluation phase. In enrollment phase signature, fingerprint and user name are stored on database. In evaluation phase, system compares the user signature, fingerprint and key pattern with previously stored one.

REFERENCES

1. J. Li, A. Najmi, and R. Gray. "Image classification by a two dimensional hidden markov model". IEEE Transactions on Signal Processing, 48(2):517–533, 2000.
2. N. K. Ratha, A. W. Senior, and R. M. Bolle, "Automated biometrics," in Proc. 2nd Int. Conf. Adv. Pattern Recog., Rio de Janeiro, Brazil, pp. 445–474, , Mar. 2001.
3. Y. Komiya, T. Ohishi, and T. Matsumoto, "A pen input on line signature verifier integrating position, pressure and inclination trajectories," IEICE Trans. Inf. Syst., vol. E84 D, no. 7, pp. 833–838, Jul. 2001.
4. A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," Pattern Recognit., vol. 35, no. 12, pp. 2963–2972, 2002.
5. Espinosa Duro V, "Minutiae detection algorithm for fingerprint recognition", IEEE Transactions on Aerospace and Electronic Systems, Vol. 17 , Issue.3, pp. 7 - 10 , March 2002.
6. Y. Chen and X. Ding, "On-line signature verification using direction sequence string matching," in Proc. SPIE 2nd Int. Conf. Image Graph., Hefei, China, , vol. 4875, pp. 744–749 Jul. 2002.
7. M. Fuentes, S. Garcia-Salicetti, and B. Dorizzi, "On-line signature verification: Fusion of a hidden Markov model and a neural network via a support vector machine," in Proc. 8th Int. Workshop Frontiers Handwriting Recog., Niagara-on-the-Lake, ON, Canada, pp. 253–258 Aug. 2002.
8. B. Bhanu, X. Tan, "Fingerprint indexing based on novel features of minutiae triplets", IEEE Trans. Pattern Recog. Anal. Mach. Intell. 25(5), pp. 616–622, 2003.
9. M. Diligenti, P. Frasconi, and M. Gori. Hidden tree markov models for document image classification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(4):519–523, 2003.
10. B. Fang, C. H. Leung, Y. Y. Tang,K.W. Tse, P.C.K.Kwok, andY.K. Wong, "Off-line signature verification by tracking of feature and stroke positions," IEEE Trans. On Pattern Recognit, vol. 36, no. 1, pp. 91–101, Jan. 2003.
11. Anil Jain, Arun Ross and Salil Prabhakar, "Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 4-20,January 2004.
12. Chan, K.C. ; Moon, Y.S. ; Cheng, P.S. "Fast fingerprint verification using subregions of fingerprint images", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14 , Issue: 1 , pp. 95 – 101, Jan. 2004.
13. J. Y. Kim, D. Y. Ko, and S. Y. Na, "Implementation and enhancement of GMM face recognition systems using flatness measure," in Proc. IEEE Int. Workshop Robot Human Interact. Commun, pp. 247–251Sep. 2004.
14. Dimauro, S. Impedovo, M. G. Lucchese, R. Modugno, and G. Pirlo, "Recent advancements in automatic signature verification," in Proc. 9th Int. Workshop Frontier Handwriting Recognit, IEEE Computer. Society Press, pp. 179–184, Oct. 2004.
15. H. Ketabdar, J. Richiardi, and A. Drygajlo, "Global feature selection for on-line signature verification," in Proc. 12th IGS Conf., Salerno, Italy, pp. 59–63, Jun. 2005.
16. J. Fiérrez Aguilar, L. Nanni, J. López-Pe´nalba, J. Ortega García, and D. Maltoni, "An on-line signature verification system based on fusion of local and global information," in Proc. IEEE Int. Conf. Audio Video-Based Person Authentication, Halmstad, Sweden, pp. 523–532, Jun. 2005.
17. J. Richiardi, H. Ketabdar, and A. Drygajlo, "Local and global feature selection for on-line signature verification," in Proc. IAPR 8th ICDAR, Seoul, Korea, vol. 2, pp. 625–629, Aug. 2005.
18. A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method," Pattern Recognit. Lett., vol. 26, no. 15, pp. 2400–2408, Nov. 2005.
19. Putz-Leszczyska, "On-line signature verification using dynamic time warping with positional coordinates," in Proc. SPIE Int. Soc. Opt. Eng., Wilga, Poland, vol. 6347, no. 2, pp. 634 724-1–634 724-08, Oct. 2006.
20. Schaumont, P. ; Hwang, D. ; Shenglin Yang ; Verbauwhede, "Multilevel Design Validation in a Secure Embedded System", IEEE Transactions on Computers, Vol. 55 , Issue. 11, pp. 1380 – 1390, Nov 2006.
21. T. Ahonen, A. Hadid, and M. Pietikainen, —Face description with local binary patterns: Application to face recognition, IEEE Trans. Pattern Anal. Machine Intell., vol. 28, no. 12, pp. 2037–2041, Dec. 2006.
22. M. Faúndez-Zanuy, "On-line signature recognition based on VQ-DTW," Pattern Recognit., vol. 40, no. 3, pp. 981–992, Mar. 2007.
23. S. Impedovo and G. Pirlo, "Verification of handwritten signatures: An overview," in Proc. 14th Int. Conf. Image Anal. Process. pp. 191–196, Sep. 2007.
24. B. Ly Van, S. Garcia-Salicetti, and B. Dorizzi, "On using the Viterby path along with HMM likelihood information for online signature verification," IEEE Trans. Syst., Man, Cybern. Part B: Cybern., vol. 37, no. 5, pp. 1237–1247, Oct. 2007.
25. J. Fierrez-Aguilar, J. Ortega-García, D. D. Ramos, and J. Gonzalez-Rodríguez,

"HMM-based on-line signature verification: Feature extraction and signature modeling," Pattern Recognit. Lett., vol. 28, no. 16, pp. 2325–2334, Dec. 2007.

26. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," IEEE Trans. Syst., Man, Cybern.—Part C: Appl. Rev., vol. 38, no. 5, pp. 609–635, Sep. 2008.
27. O. Miguel-Hurtado, L. Mengibar-Pozo, and A. Pacut, "A new algorithm for signature verification system based on DTW and GMM," in Proc. 42nd. Annu. IEEE Int. Carnahan Conf. Security Technol, pp. 206–213, Oct. 2008.
28. O. Miguel-Hurtado, L. Mengibar-Pozo, and A. Pacut, "A new algorithm for signature verification system based on DTW and GMM," in Proc. 42nd. Annu. IEEE Int. Carnahan Conf. Security Technol., pp. 206–213, Oct. 2008.
29. Gruber C, Gruber T, Krinninger S, Sick B, "Online Signature Verification With Support Vector Machines Based on LCSS Kernel Functions", IEEE transaction on System, Man, and Cybematics, Part B: Cybemetics, Vol. 40, PP. 1088 – 1100, June 2010.
30. Y. Komiya, T. Ohishi, and T. Matsumoto, "A pen input on line signature verifier integrating position, pressure and inclination trajectories," IEICE Trans. Inf. Syst., vol. E84 D, no. 7, pp. 833–838, Jul. 2010.
31. D. Impedovo and G. Pirlo, "On-line signature verification by stroke-dependent representation domains," in Proc. 12th ICFHR, Kolkata, India, pp. 623–627, Nov. 2010.
32. M. Fons, F. Fons, and E. Cantó-Navarro, "Fingerprint image processing acceleration through run-time reconfiguration hardware," IEEE Trans. Circuits Syst. II: Exp. Briefs, vol. 57, no. 12, pp. 991–995, Dec. 2010.
33. M. López-García, J. Daugman, and E. Cantó-Navarro, "Hardware-software co-design of an iris recognition algorithm," IET Inf. Security, vol. 5, no. 1, pp. 60–68, Apr. 2011.
34. Monmasson, L. Idkhajine, M. N. Cirstea, I. Bahri, A. Tisan, and M. W. Naouar, "FPGAs in industrial control applications," IEEE Trans. Ind. Inf., vol. 7, no. 2, pp. 224–243, May 2011.
35. Nanni, L. ; Brahnam, S. ; Lumini, A."Biohashing applied to orientation-based minutia descriptor for secure fingerprint authentication system", IEEE Electronics Letters, Vol. 47, Issue: 15 , pp. 851 – 853, July 2011.
36. M. Fons, F. Fons, E. Cantó-Navarro, and M. López-García, "FPGA based personal authentication using fingerprints," J. Signal Process. Syst., vol. 66, no. 2, pp. 153–189, Feb. 2012.
37. S. Jin, D. Kim, T. T. Nguyen, D. Kim,M. Kim, and J. W. Jeon, "Design and implementation of a pipelined data path for high-speed face detection using FPGA," IEEE Trans. Ind. Inf., vol. 8, no. 1, pp. 158–167, Feb. 2012.
38. Miguel A. Ferrer, J. Francisco Vargas, Aythami Morales, and Aarón Ordóñez, ―Robustness of Offline Signature Verification Based on Gray Level Features‖. IEEE Transactions on Information Forensics and Security, Vol. 7, No. 3, June 2012.
39. M. Erbilek and M. Fairhurst, "Framework for managing ageing effects in signature biometrics," IET Biometr., vol. 1, no. 2, pp. 136–147, Jun. 2012.
40. Enrique Argones Rúa,, José Luis Alba Castro, M "Online Signature Verification Based on Generative Models", IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, Vol. 42, No. 4, pp 1231 - 1242 August 2012.
41. J. Liu-Jiménez, R. Sánchez-Reillo, L. Mengibar-Pozo, and O. Miguel Hurtado, "Optimisation of biometric ID tokens by using hardware/software co-design," IET Biometrics, vol. 1, no. 3, pp. 168–177, Sep. 2012.
42. Sheng Li ; Kot, A.C.," Fingerprint Combination for Privacy Protection", IEEE Transactions on Information Forensics and Security, Vol. 8, Issue: 2 , pp. 350 – 360, December 2012.
43. R. Ramos-Lara, M. López-García, E. Cantó-Navarro, and L. Puente- Rodriguez, "Real-Time speaker verification system implemented on reconfigurable hardware," J. Signal Process. Syst., vol. 71, no. 2, pp.89–103, May 2013.
44. Eric Monmasson , Marcian Cirstea, "Guest Editorial Special Section on Industrial Control Applications of FPGAs" IEEE Transactions on Industrial Informatics, Vol. 9, No. 3, pp 1250-1252, August 2013.
45. Mariano lópez-garcía, Rafael ramos-lara, Oscar miguel-hurtado, and Enrique cantó-navarro, "Embedded system for biometric online signature verification", IEEE Transactions on Industrial Informatics, Vol. 10, No. 1, PP 491 – 501 February 2014.